Terms used **salt table password**

Found **78** of **183,790**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 78

Result page: **1** 2 3 4 next

Relevance scale

1 Password hardening based on keystroke dynamics

Fabian Monrose, Michael K. Reiter, Susanne Wetzel

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.01 MB)

Additional Information: full citation, abstract, references, citings, index terms

We present a novel approach to improving the security of passwords. In our approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both online and offline attackers. In addition, our scheme automatically adapts to gradual changes in a user's typing patterns while maintaining the s ...

2 High dictionary compression for proactive password checking

Francesco Bergadano, Bruno Crispo, Giancarlo Ruffo

November 1998 **ACM Transactions on Information and System Security (TISSEC)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: pdf(141.89 KB)

Additional Information: full citation, abstract, references, citings, index terms, review

The important problem of user password selection is addressed and a new proactive password-checking technique is presented. In a training phase, a decision tree is generated based on a given dictionary of weak passwords. Then, the decision tree is used to determine whether a user password should be accepted. Experimental results described here show that the method leads to a very high dictionary compression (up to 1000 to 1) with low error rates (of the order of 1%). A prototype implementat ...

Keywords: access control, decision trees, password selection, proactive password checking

3 Moderately hard, memory-bound functions

Martin Abadi, Mike Burrows, Mark Manasse, Ted Wobber

May 2005 **ACM Transactions on Internet Technology (TOIT)**, Volume 5 Issue 2

Publisher: ACM Press

Full text available:

Additional Information:

pdf(285.15 KB) full citation, abstract, references, index terms

A resource may be abused if its users incur little or no cost. For example, e-mail abuse is rampant because sending an e-mail has negligible cost for the sender. It has been suggested that such abuse may be discouraged by introducing an artificial cost in the form of a moderately expensive computation. Thus, the sender of an e-mail might be required to pay by computing for a few seconds before the e-mail is accepted. Unfortunately, because of sharp disparities across computer systems, this appro ...

Keywords: Spam

4 Accelerators: Accelerating the secure remote password protocol using reconfigurable hardware

Peter Groen, Panu Hämäläinen, Ben Juurlink, Timo Hämäläinen
April 2004 **Proceedings of the 1st conference on Computing frontiers**
Publisher: ACM Press
Full text available: pdf(182.13 KB) Additional Information: full citation, abstract, references, index terms

The Secure Remote Password (SRP) protocol is an authentication and key-exchange protocol suitable for secure password verification and session key generation over insecure communication channels. The modular exponentiations involved, however, are very time-consuming, causing slow log-on procedures. This work presents the design of a hardware accelerator that performs modular exponentiation of very wide integers. The experimental platform is tutwlan, a Wireless Local Area Network (wl ...

Keywords: WLAN, authentication, hardware acceleration, modular exponentiation, reconfigurable hardware, secure remote password protocol

5 Security through the eyes of users: A convenient method for securely managing passwords

J. Alex Halderman, Brent Waters, Edward W. Felten
May 2005 **Proceedings of the 14th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(187.07 KB) Additional Information: full citation, abstract, references, index terms

Computer users are asked to generate, keep secret, and recall an increasing number of passwords for uses including host accounts, email servers, e-commerce sites, and online financial services. Unfortunately, the password entropy that users can comfortably memorize seems insufficient to store unique, secure passwords for all these accounts, and it is likely to remain constant as the number of passwords (and the adversary's computational power) increases into the future. In this paper, we propose ...

Keywords: password security, website user authentication

6 Security Issues in the ABELS System for Linking Distributed Simulations

G. Ayorkor Mills-Tettey, Linda F. Wilson
March 2003 **Proceedings of the 36th annual symposium on Simulation**
Publisher: IEEE Computer Society
Full text available: pdf(478.65 KB) Additional Information: full citation, abstract, index terms

The Agent-Based Environment for Linking Simulations(ABELS) framework is designed to allow physically distributedsimulations and other data resources to form a"data cloud" for the exchange of information. In particular,it uses a distributed brokering system to facilitate dynamiclinkings between independently-designed, autonomous

participants,without requiring the use of stringent standardsto which participants must conform. This paper discussesvarious challenges in developing a security framework ...

7 Attacking passwords and bringing down the network: Fast dictionary attacks on passwords using time-space tradeoff

Arvind Narayanan, Vitaly Shmatikov

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

Publisher: ACM Press

Full text available: pdf(189.89 KB) Additional Information: full citation, abstract, references, index terms

Human-memorable passwords are a mainstay of computer security. To decrease vulnerability of passwords to brute-force dictionary attacks, many organizations enforce complicated password-creation rules and require that passwords include numerals and special characters. We demonstrate that as long as passwords remain human-memorable, they are vulnerable to "smart-dictionary" attacks even when the space of potential passwords is large.Our first insight is that the distribution of letters in easy-to- ...

Keywords: Markov models, cryptanalysis, dictionary attack, passwords, time-space, tradeoff

8 Regaining single sign-on taming the beast

Divyangi Anchan, Mahmoud Pegah

September 2003 **Proceedings of the 31st annual ACM SIGUCCS conference on User services**

Publisher: ACM Press

Full text available: pdf(217.34 KB) Additional Information: full citation, abstract, references, index terms

It has been our effort at Ringling school to provide our campus community with the capability to uniformly access resources across multiple platforms. Empowering the user with a single sign-on capability has multifold benefits. It greatly improves user experience and relieves the user from the burden of remembering multiple user-id and password pairs. On the administrative side, help desk costs are noticeably reduced and security improved, as users are not tempted to 'store' multiple passwords i ...

Keywords: LDAP, RPC, account synchronization, active directory (AD), active directory service interfaces (ADSI), password synchronization, single sign-on

9 Security procedures effects on network communication: Password policy: the good, the bad, and the ugly

Wayne C. Summers, Edward Bosworth

January 2004 **Proceedings of the winter international synposium on Information and communication technologies WISICT '04**

Publisher: Trinity College Dublin

Full text available: pdf(73.64 KB) Additional Information: full citation, abstract, references

"We're secure! We use passwords!" How many of us have heard this claim? Or even -- "We're secure! We have a password policy!" Using a password or having a password policy in today's world of computing is not enough. Passwords provide a first line of defense in most cases, but there is much more. "A recent survey by Rainbow Technologies Inc. indicates that the use of insecure passwords can be costly -- and potentially risky -- for corporate data. "[Rosencrance] This paper focuses on the use of pa ...

10 Password security: a case history

Robert Morris, Ken Thompson
November 1979 **Communications of the ACM**, Volume 22 Issue 11
Publisher: ACM Press
Full text available: pdf(446.89 KB) Additional Information: full citation, abstract, references, citings

This paper describes the history of the design of the password security scheme on a remotely accessed time-sharing system. The present design was the result of countering observed attempts to penetrate the system. The result is a compromise between extreme security and ease of use.

Keywords: computer security, operating systems, passwords

11 OpenLDAP everywhere
Craig Swanson, Matt Lung
December 2002 **Linux Journal**, Volume 2002 Issue 104
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(23.52 KB) Additional Information: full citation, abstract, index terms

A single company-wide directory service offers mail address lookup and file sharing to Linux and Windows users.

12 Password management, mnemonics, and mother's maiden names: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords
Furkan Tari, A. Ant Ozok, Stephen H. Holden
July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**
Publisher: ACM Press
Full text available: pdf(131.75 KB) Additional Information: full citation, abstract, references, index terms

Previous research has found graphical passwords to be more memorable than non-dictionary or "strong" alphanumeric passwords. Participants in a prior study expressed concerns that this increase in memorability could also lead to an increased susceptibility of graphical passwords to shoulder-surfing. This appears to be yet another example of the classic trade-off between usability and security for authentication systems. This paper explores whether graphical passwords' increased memorability neces ...

Keywords: authentication, graphical passwords, human factors, password security, shoulder surfing, social engineering, usable security

13 Password Management and Digital Signatures: The BiBa one-time signature and broadcast authentication protocol
Adrian Perrig
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**
Publisher: ACM Press
Full text available: pdf(268.66 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce the *BiBa signature* scheme, a new signature construction that uses one-way functions without trapdoors. BiBa features a low verification overhead and a relatively small signature size. In comparison to other one-way function based signature schemes, BiBa has smaller signatures and is at least twice as fast to verify (which probably makes it one of the fastest signature scheme to date for verification). On the downside, the BiBa public key is large, and the signature generation ...

Keywords: broadcast authentication, one-time signature, signature based on a one-way function without trapdoor, source authentication for multicast

14 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Publisher: ACM Press

Full text available: pdf(507.57 KB) Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

15 Password management, mnemonics, and mother's maiden names: Passpet: convenient password management and phishing protection

Ka-Ping Yee, Kragen Sitaker

July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press

Full text available: pdf(479.35 KB) Additional Information: full citation, abstract, references, index terms

We describe Passpet, a tool that improves both the convenience and security of website logins through a combination of techniques. Password hashing helps users manage multiple accounts by turning a single memorized password into a different password for each account. User-assigned site labels (petnames) help users securely identify sites in the face of determined attempts at impersonation (phishing). Password-strengthening measures defend against dictionary attacks. Customizing the user interfac ...

16 Comparing information without leaking it

Ronald Fagin, Moni Naor, Peter Winkler

May 1996 **Communications of the ACM**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(344.25 KB) Additional Information: full citation, references, citings, index terms

17 Password cracking: a game of wits

Donn Seeley

June 1989 **Communications of the ACM**, Volume 32 Issue 6

Publisher: ACM Press

Full text available: pdf(488.03 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The following report has been gleaned from "A Tour of the Worm," an in-depth account of the November Internet infection. The author found the worm's crypt algorithm a frustrating, yet engaging, puzzle.

18 Keystroke analysis of free text

Daniele Gunetti, Claudia Picardi

August 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 3

Publisher: ACM Press

Full text available: pdf(277.07 KB) Additional Information: full citation, abstract, references, index terms

Keystroke dynamics can be useful to ascertain personal identity even *after* an authentication phase has been passed, provided that we are able to deal with the typing rhythms of free text, chosen and entered by users without any specific constraint. In this paper we present a method to compare typing samples of free text that can be used to verify personal identity. We have tested our technique with a wide set of experiments on 205 individuals, obtaining a False Alarm Rate of less than 5&p ...

Keywords: Biometric techniques, identity verification, keystroke analysis of free text

19 Unified login with pluggable authentication modules (PAM)

Vipin Samar

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.12 MB) Additional Information: full citation, references, index terms

20 Password auditing applications

Randy Cisneros, Desiree Bliss, Mario Garcia

April 2006 **Journal of Computing Sciences in Colleges**, Volume 21 Issue 4

Publisher: Consortium for Computing Sciences in Colleges

Full text available: pdf(185.70 KB) Additional Information: full citation, abstract, references, index terms

A goal of computer system security is to prevent an attack, and authentication mechanisms can prevent a compromise on parts of a system. Most if not all forms of access are granted based on a single authentication scheme, and passwords are currently the most widely used authentication mechanism. Weak passwords have been cited by experts from SANS, industry, government, and academia as one of the most critical security threats to computer networks. However, various applications are available toda ...

Results 1 - 20 of 78 Result page: **1** 2 3 4 next